Morven Park Primary School

Online Safety Policy

2026-2027

Introduction and Aims

Morven Park Primary School recognises that digital technologies are an essential part of children's lives, both within school and at home. Used well, they enhance learning, communication and creativity. Used inappropriately, they may expose children and adults to risk.

This Online Safety Policy:

- sets out how we keep pupils, staff and the wider school community safe when using digital technologies (including AI tools)
- supports the school's wider safeguarding, behaviour and anti-bullying policies
- provides clear expectations and procedures for all users of school systems and services

Online safety includes, but is not limited to:

- use of the internet and web-based services
- digital communication (email, messaging, social media, video conferencing)
- use of mobile phones, tablets and other personal devices
- use of digital and video images
- data protection and privacy
- use of Artificial Intelligence (AI) tools and platforms

The Four Areas of Online Safety Risk (4Cs)

In line with Keeping Children Safe in Education, Morven Park Primary School recognises that online safety risks can be categorised into four areas:

- Content – being exposed to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, for example peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, for example making, sending and receiving explicit images, online bullying and inappropriate online behaviour.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and financial scams.

The school will ensure that its online safety education, safeguarding procedures, filtering and monitoring arrangements and response to incidents take account of all four areas of risk.

Development of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher/Deputy Safeguarding Lead – Mr Mark Watson
- Designated Safeguarding Lead – Mrs Alisa Murphy
- Deputy Safeguarding Lead – Nicky Goodall and Nicola Lomas
- Online Safety Coordinators – Miss Ellie Mobbs and Miss Reagan Hurt
- Governors

Schedule for Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by:	*Ellie Mobbs & Reagan Hurt*
Monitoring will take place at regular intervals:	*Once a year*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Once a year.*

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*5th September 2027*
Should serious online safety incidents take place, the following external agencies may be informed in line with our Safeguarding and Child Protection Policy and local procedures: *– Local Authority Designated Officer (LADO), where allegations involve staff* *– Local authority children's social care / safeguarding partnership* *– Police* *– CEOP (Child Exploitation and Online Protection Command)*	

The school will monitor the impact of the policy using:

- Logs of reported incidents - CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Legislation and Guidance

This policy takes account of, and should be read alongside, the most recent versions of:

- Keeping Children Safe in Education (DfE, current version as updated from time to time)
- The Online Safety Act 2023
- Education Act 2011 and Education and Inspections Act 2006
- Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025
- Prevent Duty guidance
- DfE guidance "Meeting digital and technology standards in schools and colleges: Filtering and monitoring" (current version)
- ICO and DfE guidance on the use of Artificial Intelligence (AI) in education
- Local Authority safeguarding procedures

Where there is any conflict between this policy and statutory guidance, the statutory guidance takes precedence.

Scope of the Policy

This policy applies to all members of Morven Park Primary School (including staff, pupils, volunteers, parents / carers, visitors, governors) who have access to and are users of school digital technology systems, both in and out of Morven Park.

The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Morven Park deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Morven Park.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *Online Safety Governor*. The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Co-ordinators
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Headteacher

- Mark Watson has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to Ellie Mobbs and Reagan Hurt.
- Mark Watson and Alisa Murphy should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Mark Watson is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Coordinator

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (this is through CPOMS)
- Log any online safety issues on CPOMS under the 'E Safety category' whether this has been in school, or through conversations with parents, or other
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings with committee of Governors
- Reports regularly to Senior Leadership Team

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they report any suspected misuse or problem to Mark Watson, Alisa Murphy and Ellie Mobbs for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- log any online safety issues on CPOMS under the 'E Safety Category' whether this has been in school, or through conversations with parents, or other

Designated Safeguarding Lead (Mrs Alisa Murphy)

Should be trained in Online Safety issues and be aware of the potential for serious child safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Pupils:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Morven Park's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and parent workshops. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught, in an age-appropriate way, about emerging online harms, including misinformation, manipulated and AI-generated content and images (including deepfakes), harmful online influences and inappropriate content. Pupils will be taught how to recognise these risks, respond safely and know when and where to seek help.
- Online safety education will be adapted to meet the needs and vulnerabilities of individual pupils, including pupils with Special Educational Needs and Disabilities (SEND). The school recognises that some pupils may be more vulnerable to online risks, including bullying, grooming, exploitation and radicalisation. Appropriate support, teaching and reasonable adjustments will be provided to help pupils recognise risks, stay safe online and know how and where to seek help.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, website,*
- *Parent workshops*
- *High profile events. E.g. Safer Internet Day*
- *Reference to the relevant web E.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers*

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy.
- All staff will receive training on their roles and responsibilities in relation to filtering and monitoring. This will include understanding how the school's filtering and monitoring systems support safeguarding, how to recognise when systems may not be working effectively, and how and to whom concerns should be reported. Staff knowledge will be updated at least annually and whenever there are significant changes to the school's systems or procedures.
- Basic awareness of AI risks and opportunities.

Training – Governors

Governors should take part in online safety training sessions, with particular importance for those who are members of any safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in school training / information sessions for staff or parents.
- Briefings on new legislation and emerging technologies, including AI.

Technical – Equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Ellie Mobbs who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when/ if needed.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to Ellie Mobbs.
- Ellie Mobbs and Reagan Hurt are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Our filtering and monitoring arrangements will be reviewed at least annually, and whenever there are significant changes to the school's systems or identified risks, to ensure that they meet the current DfE Filtering and Monitoring Standards and Keeping Children Safe in Education requirements.

The review will be led by the member of the Senior Leadership Team responsible for filtering and monitoring, supported by the Designated Safeguarding Lead (DSL) and the school's IT support/provider. The review will consider the effectiveness of the school's filtering and monitoring arrangements and whether they are appropriate for the age and needs of pupils and the risks within our setting.

Checks will include filtering and monitoring arrangements on all school-managed internet-connected devices and systems, and across relevant locations within the school. A record of the review and checks undertaken, any issues identified and any actions required will be maintained.

All staff will understand their roles and responsibilities in relation to filtering and monitoring and will know how to report concerns or instances where filtering or monitoring may not be working as expected.

Filtering and monitoring arrangements will also take account of emerging technologies, including generative AI. Systems will be configured, as far as technically possible and appropriate, to manage access to AI tools and to identify and respond to harmful or inappropriate AI-related content.

Mobile Technologies and Personal Devices

Morven Park Primary School provides a mobile phone-free environment for pupils during the school day, in line with current DfE guidance. Pupils should not use or access mobile phones during the school day. Where pupils need to bring a mobile phone to school, it must be stored securely in accordance with school procedures and must not be accessed during the school day. Exceptions may be agreed by the Headteacher where there is a specific individual need, such as a medical requirement or other exceptional circumstance.

- Mobile technology devices may be school-owned / provided or personally owned and might include smartphones, tablets, laptops or other technology that can use the school's wireless network.
- All users should understand that the primary purpose of using mobile / personal devices in school is educational.
- The mobile technologies policy will be consistent with and related to other school policies, including:
    - Safeguarding Policy
    - Behaviour Policy
    - Anti-Bullying Policy
    - Acceptable Use Policy
    - policies on theft or malicious damage

- Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education (e.g. through Kapow and Purple Mash schemes).

Use of digital and video images

The school will:

- inform and educate users about the risks associated with the taking, use, sharing, publication and distribution of images
- ensure that staff explain to pupils the risks of publishing personal images on the internet (e.g. social networking sites)
- obtain written permission from parents / carers before photographs of pupils are published on the school website, social media or in the local press
- ensure that images are used only for the intended purpose and stored securely in line with data protection requirements

Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025. The DSL will assess data protection risks when using online services and AI tools, particularly where pupil work or personal data may be uploaded. Any use of AI must comply with the Data Protection Policy and relevant guidance.

Communications

The school will:

- use the official Morven Park email service as the norm for communication involving pupils and parents / carers
- ensure personal email accounts are not used for school business
- restrict pupil access to communications technologies according to age and purpose

Good practice:

- Users must immediately report any communication that makes them feel uncomfortable or appears offensive, discriminatory, threatening or bullying and must not respond.
- All digital communication between staff and pupils or parents / carers must be professional in tone and content and take place only through official, monitored school systems.
- Whole-class email addresses may be used at Key Stage 1, while Key Stage 2 pupils may be provided with individual school email addresses for educational use.
- Pupils will be taught about online safety issues, including risks of sharing personal details and strategies to deal with inappropriate communications.
- Personal staff information should not be posted on the school website; only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

The school has a duty of care to provide a safe learning environment for pupils and staff. Staff members who misuse social media may bring the school into disrepute and/or breach professional standards.

The school will:

- ensure personal information is not published without consent
- provide training including acceptable use, social media risks, checking privacy settings, data protection and reporting issues
- provide clear reporting guidance, including responsibilities, procedures and sanctions
- carry out risk assessment where appropriate

Staff must ensure that:

- no reference is made in personal social media to pupils, parents / carers or other staff
- they do not discuss personal matters relating to members of the school community on social media
- personal opinions are not attributed to the school or Local Authority
- privacy / security settings on personal profiles are regularly checked

Use of Artificial Intelligence (AI)

For the purposes of this policy, "AI tools" include:

- generative AI (e.g. tools that create text, images, audio, video, code)
- AI-enabled chatbots and virtual assistants
- AI-powered educational apps and platforms

Principles

- AI must be used to support teaching, learning and workload, not replace professional judgement.
- Staff must review and check AI-generated content before sharing or using it with pupils.
- AI must not be used to create or share harmful, discriminatory or age-inappropriate content.
- AI must not be used in ways that undermine assessment integrity (e.g. completing pupils' work for them).

Age-Appropriateness and Access

- The school will respect age restrictions for AI tools and apps.
- Pupils will only access AI tools that are age-appropriate and approved by the school.
- Use of AI by pupils will be supervised and clearly linked to learning objectives.
- Parents will be informed where the use of AI tools for homework or projects is encouraged or expected.

Any pupil-facing AI tools must:

- be age-appropriate and approved by the school
- be used under staff supervision
- form part of a planned learning activity which includes explicit teaching of AI literacy and critical evaluation of AI outputs.

Data Protection and Privacy

- Staff and pupils must not input unnecessary personal data into AI tools.
- Any use of personal data with AI must comply with UK GDPR and the school's Data Protection Policy.
- Staff must check the privacy and data-use terms of AI tools before using or recommending them with pupils.
- Concerns about data protection and AI must be reported to the DSL.

Education and Digital Literacy

Pupils will be taught:

- what AI is and how it works at an age-appropriate level
- that AI outputs can be inaccurate, biased or misleading
- how to critically evaluate AI-generated content
- how to use AI tools safely, respectfully and ethically

Staff will receive training on:

- the benefits and limitations of AI in education
- managing risks such as harmful prompts, misinformation and over-reliance on AI
- supporting pupils to use AI appropriately and in line with this policy

Use of AI tools that involves personal data or profiling of pupils or staff will be risk assessed in consultation with the DSL. Where required, a Data Protection Impact Assessment (DPIA) will be completed before use, in line with UK GDPR and ICO guidance on AI and data protection.

AI tools will not be used to make automated decisions about pupils or staff that have legal or similarly significant effects (for example, decisions about exclusion, safeguarding risk, or high-stakes assessments) without meaningful human oversight and final decision-making, in line with UK GDPR.

Dealing with Unsuitable / Inappropriate Activities

The school considers certain activities inappropriate or illegal and prohibits users from engaging in such activities using school equipment or systems, in or outside school. This includes using AI tools to generate such content.

Examples include:

- accessing, creating or sharing:
- child sexual abuse images
- grooming or sexual exploitation material
- extreme pornography

- criminally racist material
- pornography or sexually explicit content
- discriminatory material
- threatening, violent or hate content
- extremist or terrorist material
- using school systems to run a private business
- using methods to bypass or subvert filtering systems (including via AI tools)
- infringing copyright
- revealing or publicising confidential or proprietary information
- creating or propagating computer viruses or other harmful files
- downloading / uploading large files that hinder others' internet use
- unauthorised online gambling or shopping
- misusing social media, messaging apps or blogs
- using AI tools to:

    - generate harmful, abusive or explicit content
    - impersonate others
    - cheat in assignments
    - creating, sharing or threatening to share intimate images, including 'nudes' or 'semi-nudes', whether consensually or non-consensually. This includes images that have been self-generated, digitally altered or wholly generated using Artificial Intelligence (AI), including deepfakes or 'deep nudes'

Responding to Incidents of Misuse

Incidents involving the creation, sharing or threatened sharing of nudes or semi-nudes, including digitally altered or AI-generated images, will be managed in line with current UKCIS guidance and the school's Safeguarding and Child Protection Policy, with police involvement where required.

Illegal Incidents

If there is any suspicion that a website or content may contain child abuse images or other illegal material:

- do not continue to view the material
- report immediately to the Headteacher / DSL
- contact the Police and / or CEOP as appropriate
- follow Local Authority safeguarding procedures

Other Incidents

Where misuse is suspected:

- Involve more than one senior member of staff in the process.
- Use a designated computer (not accessible to pupils) that can be taken off site by the Police if necessary.
- Ensure relevant staff have appropriate access but that all sites and content visited are closely monitored and recorded.
- Record URLs of sites visited, nature of the content causing concern, dates and times, and any screenshots if appropriate (never for child sexual abuse images).
- Assess whether the concern has substance. If it does, possible actions include internal response / disciplinary procedures, Local Authority involvement or Police action.
- If content includes child abuse images or clear illegal material, stop immediately and refer to the Police.
- Isolate the computer to preserve evidence where necessary.

All steps must be carefully documented.

School Actions & Sanctions

Online safety incidents may form part of wider child-on-child abuse. We follow our Safeguarding and Child Protection Policy where there is any indication of abuse, exploitation or significant harm, including where online behaviour is involved.

Pupil Incidents

Possible sanctions include:

- discussion with class teacher
- referral to Key Stage Leader / SLT
- informing parents / carers
- temporary or permanent removal of network / internet access
- additional education / reflection work
- detention or, in serious cases, suspension / exclusion
- referral to Police or other agencies for serious or repeated incidents

Staff Incidents

Incidents involving staff may lead to:

- advice and guidance
- formal warning
- referral to Headteacher
- involvement of Local Authority / HR
- suspension and/or disciplinary action
- referral to Police for illegal activity

Conclusion

Morven Park Primary School is committed to ensuring that all members of the school community are safe and responsible users of digital technologies and AI. Through robust technical measures, a clear policy framework, education, training and partnership with parents, we aim to reduce the risks of harm, promote positive use of technology and respond swiftly, fairly and effectively to any incidents that arise.

Signed by: (Head teacher)
_____ Date:_____

Signed by: (Designated Safeguarding Lead)
_____ Date:_____

Signed by: (Governor)
_____ Date:_____

Signed by: (Online Safety Coordinator)
_____ Date:_____